Mimoto: Continuous Person-Based Verification for the Modern Cyber Battlefield

Overview

Traditional cybersecurity defenses rely on credentials, tokens, and anomaly detection — but adversaries have evolved faster than the systems protecting America's critical infrastructure. In 2024 alone, insider threats and AI-powered intrusions cost organizations over **$800 billion globally**, with **95% of breaches involving human factors** Compromised credentials, deepfakes, and "agentic AI" actors now routinely bypass MFA, PAM, and identity management tools. Meanwhile, the proliferation of AI in cyberattacks is resulting in exponential growth in the number of attacks and their sophistication.

Mimoto introduces a new defense paradigm: **Person-Based Continuous Verification**. Instead of securing *accounts*, Mimoto secures *people* — continuously verifying the real human behind every credential, account, or access point, in real time.

The Problem: Credentials Can No Longer Be Trusted

For federal cybersecurity managers, the threat landscape has shifted from network perimeter defense to continuous identity assurance. Yet current tools depend on credentials and static authentication events that attackers can easily hijack.
Key challenges include:

- **Credential Compromise & Account Takeover:** Adversaries exploit stolen or shared credentials across hybrid cloud and SaaS systems.
- **Insider Threats & Privileged Abuse:** Even authorized users may act maliciously or from unsanctioned regions, violating regulatory or security policy.
- **AI-Driven Impersonation:** Deepfakes and autonomous agents can now mimic human logins, voice, or behavioral patterns with alarming precision.
- **Regulatory Gaps:** NIST, OMB, and Zero Trust frameworks introduce significant user friction, while demanding *continuous* validation of user identity and behavior — something legacy IAM and MFA cannot provide.

The result: cyber leaders face blind spots inside their most trusted systems — where attacks unfold quietly, often by *valid users doing invalid things*.

©2025 Mimoto, Inc.

The Solution: Mimoto's Continuous Verification Platform

Mimoto's pending patented platform uses **multidimensional behavioral "fingerprints"** — a fusion of **AI-driven advanced pattern matching** and **anomaly detection** — to recognize and respond to identity misuse **the instant it occurs**.

Instead of relying on static credentials or behavioral baselines, Mimoto builds a live, multidimensional behavioral profile of each individual and continuously validates that the *person* behind every session is genuine, authorized, and acting within their sanctioned context.

Core Capabilities

- **Person-Specific Recognition:** Detects when a credential or generic account is used by anyone other than the verified individual, even when authentication is bypassed
- **Real-Time Response:** Instantly interrupts ransomware activity, data theft, or policy violations.
- **Behavioral Context Awareness:** Recognizes location, device, access pattern, and mission context to confirm legitimacy.
- **Agentic AI Detection:** Identifies and blocks bots or synthetic identities posing as human users.
- **Cloud-Agnostic Deployment:** Operates at any access point — managed endpoint, SaaS, shared workstation, or BYOD — even in air-gapped or limited-connectivity environments

---

Federal and Defense Use Cases

1. **Offshore and Remote Developers:** Verify that only contracted personnel, in an authorized location, access code repositories or mission systems — not unauthorized offshore actors or AI proxies.
2. **Privileged User Oversight ("Watching the Watchers"):** Detect and stop unauthorized activity from admin or IT staff with elevated privileges.
3. **Data Loss Prevention:** Identify who is accessing sensitive datasets — and act automatically if access context violates policy.
4. **Ransomware Prevention:** Block malicious behavior at the human level before encryption or exfiltration begins.
5. **Regulated or Classified Environments:** Add person-level continuous verification to meet compliance for financial, healthcare, or national security operations.
6. **Supply Chain and Open-Source Protection:** Detect and respond to backdoor access injected into software supply chain or open source. These capabilities directly support federal Zero Trust objectives (OMB M-22-09, NIST SP 800-207), ensuring that identity assurance extends beyond authentication to continuous verification and context-based enforcement.

©2025 Mimoto, Inc.

Why Mimoto Matters to U.S. Government Cyber Leaders

Mimoto aligns with the **Cybersecurity and Infrastructure Security Agency (CISA)** and **DoD Zero Trust** mandates for **"continuous identity evaluation."**
Its **person-based architecture** delivers what existing IAM, PAM, and MFA systems cannot — the ability to *see and stop* human or agentic activity that looks legitimate but behaves maliciously.

Key Advantages

- **Real-time, autonomous defense:** Machine-speed response prevents lateral movement and data theft.
- **Credential-independent:** Operates even if credentials, MFA, or tokens are compromised.
- **Mission adaptability:** Deployable in tactical networks, cloud workloads, and hybrid IT.
- **Privacy-preserving design:** Uses behavioral models, not biometrics, to ensure compliance with U.S. data regulations.
- **Proven and extensible:** Early adopters in financial and cyber-tech sectors have already doubled renewals, validating operational value and scalability.

Conclusion: A Shift from Access Control to Person Verification

As adversaries weaponize AI and infiltrate via trusted accounts, the next generation of federal cybersecurity must validate users continuously — not at login, but *throughout every interaction*. Mimoto's technology provides that missing layer: **real-time, behavioral verification of the individual**, enabling defense, civilian, and intelligence agencies to maintain operational trust in every digital interaction.

By moving from *"Who has access?"* to *"Who is actually behind the screen?"*, Mimoto gives U.S. cyber defenders a decisive advantage in a world where both humans and machines are capable of deception.

Contact:
Mimoto, Inc. – www.mimoto.ai
Kris Bondi, CEO & Co-Founder — kris@mimoto.ai | +1 (415) 812-3503

©2025 Mimoto, Inc.